图书情报工作
第65卷 第17期 2021年9月

加拿大隐私影响评估政策:历程、内容、分析与启示*

■ 陈美[1] 梁乙凯[2]
[1] 中南财经政法大学公共管理学院 武汉 430073 [2] 山东财经大学管理科学与工程学院 济南 250014

摘 要:[目的/意义]从政策的角度,调查加拿大隐私影响评估的政策支持,为我国隐私影响评估政策制定提供参考,为政府保护公民隐私提供工具。[方法/过程]利用文献调研和案例分析的研究方法,以加拿大为例,通过对文献资料和网站内容的调查,获取一手资料阐述加拿大隐私影响评估政策的发展历程,对政策目标、政策主体、政策内容进行梳理,并在此基础上分析加拿大隐私影响评估政策的优势和不足。[结果/结论]提出提高政策执行人员技能、尽早制定PIA政策、加强PIA政策认同的建议。
关键词:隐私影响评估 加拿大 政府开放数据 隐私风险
分类号:D035
DOI:10.13266/j.issn.0252-3116.2021.17.014

随着信息通信技术的快速发展,它提供了许多可能性并产生了许多优势。个人电脑和电信网络的使用提高了服务效率,促使我们的日常生活变得更加便捷。然而,技术也为个人隐私和自由带来了新危险,如许多情况下,传播的数据涉及自然人,与个人数据相关的数据库或文件被创建、使用、披露、出售,使得很难知道谁拥有数据以及这些人在做什么。个人不再能够控制他们的数据,使得滥用的风险也在增加。因此,需要对数据处理进行分析,以确定相应风险和影响。作为一种政府工具,"隐私影响评估"(privacy impact assessment,PIA)能评估数据控制者的活动对数据保护和个人隐私的影响,可以最大程度地降低潜在风险,并为数据控制者和数据主体在行使其权利和自由时营造更安全的环境。至少从20世纪80年代开始,随着针对技术的政策性辩论的出现,从而提出了PIA这一概念。通过将"PIA"和"政策"两个子概念结合得出,PIA政策是指政党、行政机关及相关政治团体为实现隐私影响评估而确定的相关指南和准则,包括规章、指令、高级官员的演讲和指示等。之所以选择加拿大作为PIA政策的案例研究,原因在于:一方面,从国内研究情况来看,尽管有学者围绕中外PIA标准进行研究[1],解析欧盟《通用数据保护条例》(General Data Protection Regulation,GDPR)中数据保护影响评估制度的相关规定[2],对PIA的缘起、价值、实施进行了研究[3],但尚未对加拿大PIA政策进行系统研究;另一方面,从实践的角度来看,加拿大的PIA政策相对比较完善。因此,笔者通过梳理加拿大PIA政策的发展历程,分析其政策内容,探讨政策的优缺点,以期为我国个人隐私保护和大数据治理工作提供参考。

1 加拿大PIA政策发展历程

从时间顺序来划分发展历程,能清楚呈现PIA政策的变化轨迹,并较为深刻地分析其背后的观念转变。但是,时间只是政策演变的外在表现,并不是政策演变的本质,因而也应当关注其发展程度。因此,笔者从时间顺序并结合发展程度,将加拿大PIA政策发展历程划分为3个阶段。

1.1 准备阶段

2000年5月,隐私专员办公室(Office of the Privacy Commissioner of Canada,OPC)发布《提交给议会的年度报告1999-2000》,强调了隐私关注不够所带来的后果:巨大的个人数据库、强大的计算机系统以及与省级社会计划和私营部门之间不断增长的联系相结合,引起了人们对隐私的极大关注,但如果政府没有适当地评估和减轻这种担忧,或者没有预料到公众对该计划的负面反应,最终会导致更大损失。尽管这一文

* 本文系国家自然科学基金项目"面向用户的开放政府数据使用行为机理及隐私风险控制研究"(项目编号:72004056)研究成果之一。
作者简介:陈美(ORCID:0000-0003-1333-546X),副教授,博士,E-mail:chenmei672236@163.com;梁乙凯(ORCID:0000-0002-8696-4446),副教授,博士。
收稿日期:2021-04-13 修回日期:2021-06-08 本文起止页码:142-151 本文责任编辑:徐健

件所述情况发生在以前，但它反映了联邦政府内部隐私保护的开创性时刻，针对不良隐私计划带来的风险提供了一个关键示例，而且对 PIA 过程进行概述，详情如表 1 所示：

表 1　PIA 要素[4]

要素	内涵
主体	进行评估的最佳主体应该是提出建议的公共或私营部门。尽管数据保护和隐私专员具有专业知识，但没有谁比设计产品或服务的人更了解详细的建议。它们最适合回答评估提出的问题。但是，为了保证评估的客观性，评估主体应咨询受影响的加拿大人，将完成的评估交给独立的隐私专家进行审核，然后将完成的评估提供给公众
时间	从逻辑上讲，评估应该是提案设计阶段的一部分，并且在组织决定检查其可行性时应立即进行评估。尽管可能在实施提案之前完成一些评估，但有些评估可能会在实施期间继续进行。还有一些评估可能永无止境，而且也是质量控制不可或缺的一部分
内容	虽然每次评估都会随每个提案的情况和性质而有所不同，但都应根据国际公认的信息隐私原则、适用的隐私保护法律以及受影响加拿大人的隐私期望进行评估
作法	每次评估应处理并记录以下要素：①提案：组织应彻底描述提案，详细说明其组成部分和时间表，提供背景信息，并概述提案的范围（谁以及将影响什么）；②影响：组织应描述该提案对加拿大人隐私的正面和负面影响，包括每种影响的累积性质，以及其持续时间、频率、强度、概率和范围，然后对每种影响进行分级，如低、中或高；③必要性：组织应证明提案本身、时间安排和负面影响的必要性（商业利益除外）；④合规性：组织应根据国际公认的隐私原则、适用的隐私保护法律以及受影响加拿大人的隐私期望来评估其提案；⑤替代方案和解决方案：组织应同时确定可以避免上述影响和合规性问题的替代方案，以及可以消除或减轻影响或合规性问题的解决方案

2002 年 5 月，加拿大政府颁布《隐私影响评估政策》（简称 PIA 政策）[5]，要求对所有会增加隐私风险的政府行动进行 PIA，并将分析结果以及为解决已发现的风险而建议采取的措施与 OPC 共享，以供审核和评估、评论，而且政府机构必须在其网站上发布其 PIA 的摘要[5]。该政策旨在向加拿大人保证，在针对那些计划、服务和方案的设计、实施和发展过程中会引起隐私问题的计划和服务而提出建议时，将考虑隐私原则。该政策涉及政策要求、作用和问责制、监测和监督，规定了 PIA 的开发和维护，并要求政府机构将 PIA 的结果告知隐私专员和公众。

2002 年 8 月，加拿大颁布《PIA 指南：管理隐私风险的框架》（简称 PIA 指南）[6]，包含旨在为完成 PIA 提供全面框架的指南，长达 40 页，分为六章，包括引言、目的、PIA 程序、流程概述、详细流程描述、隐私影响分析报告。具体而言，完成 PIA 的框架包括：何时需要 PIA 的检查表；PIA 目标；过程概述（资源需求、记录数据流、隐私分析、隐私影响分析报告、应对风险）；联邦项目和服务的问卷调查；针对跨区域项目和服务提供进行问卷调查；初步 PIA（Preliminary Privacy Impact Assessment，PPIA）和 PIA 内容的模型表。这一政策使得 PIA 能确保隐私原则和立法在新计划、服务或计划的整个生命周期中得到考虑和遵守，并且在适当的情况下，对于正在进行的服务进行转型或重新设计现有计划。在加拿大政府，多阶段评估由过去非正式政策转变为正式政策。具体而言，这个过程包括一个初步的隐私影响评估和以后的完整隐私影响评估。PPIA 不会像 PIA 那样全面，但将用于向部门项目经理表明提案是否存在重大隐私风险[6]。PPIA 有点像筛选工具，但也是一种缩写 PIA，类似于其他司法管辖区的隐私扫描或隐私影响声明。

2002 年 8 月，加拿大发布《PPIA 模型》，这是针对 PPIA 和 PIA 标准化生产的电子模板（PIA 报告模板）[7]。2003 年 3 月，加拿大发布《PIA 最佳实践报告》，确定在部门日常运营中实施 PIA 政策和指南的实用技巧和最佳实践[8]。2003 年 10 月，加拿大发布《PIA 电子学习工具》[9]，包括 3 个方面内容：①概述模块，对加拿大隐私权的基本原则进行回顾，并讨论隐私权保护程序的基本原理，包括关键隐私定义、加拿大隐私立法和政策回顾、PIA 的主要特点和益处、PIA 流程概述和 PIA 涉及的主要利益相关者；②管理或监督模块，旨在审查与 PIA 相关的关键概念，如立法和政策以及关键利益相关者，但比前面所述的概述模块更详细地审查整个 PIA 过程，包括从参与 PIA 项目的加拿大政府人员的"最佳实践"中获取的技巧，协调和监督 PIA 项目；③对 PPIA 或 PIA 进程提供逐步审查，如怎样写报告的执行摘要或如何使用文件更改控制表（document change control table），以及填写联邦计划和服务调查问卷，而且还提供转向《隐私法》（Privacy Act）[10]、《个人信息保护与电子文件法》（Personal Information Protection and Electronic Documents Act，PIPEDA）[11]，甚至关键术语定义等内容的链接。

这一阶段主要侧重于政策规划及形成，即隐私保护这一问题发生、政策问题认定及规划方案，并将方案予以合法化，而产生正式政策的过程。例如，隐私专员办公室发布报告，自上而下推动，提出隐私保护这一政策问题，很快被政府所接纳，并积极推进。

1.2　实施阶段

2004 年 5 月，加拿大发布《PIA 审计指南》，包括几个方面内容：介绍政策要求以及相关信息和关键来源，以了解 PIA 过程的基本知识；提供背景信息，以扩大读者对完成、审查和批准 PIA 所涉及的关键利益相关者责任的理解；提出审计目标和标准内部审计师可以使

用基于风险的审计方法制定定制的审计计划[12]。

2008 年 4 月 1 日,《社会保险号码(SIN)指令》生效,取代了 1993 年所颁布的《隐私和数据保护政策》[13]中的“与社会保险号码相关的政策要求”的内容。1993 年,加拿大颁布《隐私和数据保护政策》,该政策的目标是:确保政府机构有效和一致地适用《隐私法》和《隐私条例》(Privacy Regulations)[14]的规定;确保用于行政目的的个人信息的数据匹配和数据链接符合上述法律的要求;将为行政目的征收和使用社会保险号码(SIN)的范围限制在特定法案、法规和方案允许的范围内,并为其设定征收条件。《社会保险号码(SIN)指令》的附录 B 部分规定了获得政策批准的三个步骤:初步评估、分析和咨询、寻求批准。在第二步提到,在寻求财政委员会主席(President of the Treasury Board)的批准之前,需要进行以下过程:向财政委员会秘书处(Treasury Board of Canada Secretariat,TBS)的信息和隐私政策司提交一份与新收藏的完整的 PIA 报告;根据《隐私保护政策》第 6.2.12 条和《隐私法》第 9(4)条,通知隐私专员。

2010 年 4 月 1 日,加拿大财政委员会秘书处颁布了一项关于 PIA 的新指令《PIA 指令》[15]。该指令取代了自 2002 年 5 月 2 日生效的《PIA 政策》和 1993 年所颁布的《隐私和数据保护政策》中的数据匹配部分。这个新指令适用于政府机构,但不适用于新立法的制定。该指令指出,加拿大政府致力于确保:隐私保护是涉及个人信息的计划和活动的初始制定和后续管理的核心考虑因素。

2011 年 3 月,隐私专员办公室(OPC)发布了一份指导文件《期望:向加拿大隐私专员办公室提交 PIA 的指南》,以阐明当机构提交最终的 PIA 报告时,其对政府应提供的信息类型和深度的期望。尽管加拿大财政部秘书处制定的政策要求提供 PIA,但隐私专员呼吁将法律《隐私法》作为一项更广泛的改革的一部分,而且要求进行这项改革。隐私专员支持《PIA 指令》,但认为将其转化为法律,那么会具有更强的效力。

这一阶段不仅关注 PIA 政策问题的性质、政策目标,以及政策方案的可行性及可能后果,而且还关注 PIA 政策与隐私保护法之间的互动。政策与法律之间相互联动,呈现出一体两面的互动关系。一方面,政策法律化即政策转换成立法:将 PIA 政策立法;另一方面,试图通过法律《隐私法》来影响、改变人们的制度性行为,使人们的行为朝着决策者、立法者所希望的方向发展,即法律是实现 PIA 政策目标的工具。

1.3 发展阶段

2020 年 3 月 13 日至 2020 年 9 月 30 日,《隐私保护临时政策》[16]生效,取代了 2018 年 7 月 1 日发布的《隐私保护政策》。根据该文件第 4.2.14 条,政府机构负责人确保在适用时制定、维护和发布 PIA 和多机构 PIA;但是,在紧急的新型冠状病毒肺炎(COVID-19)相关倡议下,副职领导或其助理副职代表可以行使酌处权,针对新的或经过实质性修改的方案完成隐私合规性评估,以代替进行完整的 PIA。如果针对在 2020 年 12 月 31 日之后继续进行的计划行使自由裁量权,那么必须在 2021 年 6 月 30 日之前完成完整的 PIA。

2020 年 3 月 13 日至 2020 年 9 月 30 日,《隐私惯例暂行指令》[17]生效,取代了 2014 年 5 月 6 日发布的《隐私惯例指令》。根据该文件第 6.1.4 条,政府机构负责人要向财政委员会秘书处提交每个新 PIB(个人信息库)的注册或终止现有 PIB 的请求,并确保请求随附以下信息:在要求注册新的 PIB 的情况下,该法案第 11(1)(a)(i)至(vi)项中所述的 PIB 的所有要素,以及已完成并获得批准的核心隐私影响评估。PIB 是指个人信息的集合或分组。

2020 年 3 月 13 日至 2020 年 9 月 30 日,《PIA 暂行指令》[17]生效,取代《PIA 指令》。

2020 年 3 月,《期望:向加拿大隐私专员办公室提交 PIA 的指南》这一文件得到更新,作为 PIA 流程的一部分而为联邦公共部门机构提供了有关如何遵守《隐私法》和有效管理隐私风险的指南。它提出了关键概念,并提出了机构如何评估其计划和活动,包括要考虑的法律要求和隐私原则[18]。

随着信息技术的发展,需要对原有 PIA 政策进行完善,并发挥 PIA 政策撬动和引导作用。因此,这个阶段关注对 PIA 政策进行调整,从而不仅能协调政策目标与政策方案的关系,还能够保证 PIA 政策的连贯性。具体而言,加拿大 PIA 政策调整有不同的形式,如政策撤换(《隐私保护临时政策》《隐私惯例暂行指令》《PIA 暂行指令》)及政策更新(《期望:向加拿大隐私专员办公室提交 PIA 的指南》)。

2 加拿大 PIA 政策体系分析

2.1 政策目标

PIA 的特定目标包括:与公民建立信任和信心;增进对隐私问题的认识和了解;确保隐私保护是项目目标和活动的初始框架中的关键考虑因素;确定对隐私问题的明确责任制;减少在计划或服务实施后必须终

止或进行实质性审核以符合隐私要求的风险；为决策者提供必要的信息，以便他们根据对隐私风险的了解以及减轻这些风险的选择来做出明智的政策、系统设计或采购决策；提供有关业务流程和个人信息流的基本文档，供部门工作人员共同使用和查看，并作为与利益相关者进行磋商的基础[6]。

2.2 政策主体

不同的政策主体可以参与制定 PIA 政策。这些主体从对隐私保护问题的感知开始，使其成为政府行动的问题，将其列入政府的议程以供考虑，最后确保相关的政府行动，而且所有这些都需要以政府行动的形式让利益相关者参与。就加拿大而言，隐私专员办公室（OPC）和财政委员会（Treasury Board）是 PIA 政策主体，不仅了解 PIA 在推动本国发展目标方面的作用，而且实施相关政策。

2.2.1 隐私专员办公室（OPC）

OPC 不仅为个人提供有关个人信息保护的建议和信息，而且还执行《隐私法》和《个人信息保护与电子文件法》（PIPEDA）两项联邦隐私法，这两部法律规定了联邦政府机构和某些企业必须如何处理个人信息的规则[19]。例如，《隐私法》涵盖了联邦政府如何处理个人信息；PIPEDA 是加拿大的私营部门隐私法，涵盖企业如何处理个人信息。根据《隐私法》[10]，加拿大隐私专员有权检查受该法案约束的政府机构对个人信息的收集、使用、披露以及保留和处置。可见，隐私专员是执行隐私立法要求的核心人物，负责保护和促进加拿大境内个人的隐私权利。为了确保对提议或重新设计的程序和服务固有的隐私影响有全面和最新的了解，OPC 的代表还要参与 PPIA 或 PIA 的最早开发阶段。通过与机构官员合作审查文档，他们可以为机构提供建议和指导，并确定那些旨在应对潜在隐私风险的解决方案。在收到最终的 PIA 后，隐私专员可以酌情向机构负责人或副职领导提供建议[5]。为了推动 PIA 政策，加拿大隐私专员或其工作人员针对 PIA 发表了一系列讲话，如表 2 所示：

表 2　OPC 关于 PIA 的演讲

时间	演讲者	演讲题目	活动
2002 年 5 月 8 日	隐私影响评估代理总监 Claude Beaulé	《隐私影响评估》[20]	部门间隐私和政府在线工作组
2004 年 3 月 10 日	隐私专员 Stuart Bloomfield	《隐私影响评估的作用》[21]	政府信息管理第二届年度论坛
2011 年 9 月 28 日	助理隐私专员 Chantal Bernier	《隐私影响评估：隐私保护新形势下的 GPS》[22]	隐私信息管理局第二届年度隐私研讨会
2013 年 6 月 18 日	助理隐私专员 Chantal Bernier	《面对漏洞：作为生态系统的隐私和安全》[23]	2013 年海事访问和隐私会议
2013 年 9 月 26 日	助理隐私专员 Chantal Bernier	《基于风险的问责制和合规性方法》[24]	第 35 届国际数据保护和隐私专员会议
2014 年 12 月 10 日	隐私专员 Daniel Therrien	《作为隐私倡导者一起工作》[25]	ATIP 社区会议
2016 年 4 月 20 日	隐私专员 Daniel Therrien	《隐私与网络安全的互联世界》[26]	国家安全从业者项目网络安全会议
2020 年 3 月 9 日	隐私专员 Daniel Therrien	《现代化联邦隐私法，以更好地保护加拿大人》[27]	联邦获得信息和隐私权社区会议

2.2.2 财政委员会（Treasury Board）

对公共机构进行 PIA 的关键主体是财政委员会。尽管联邦立法没有明确规定应进行隐私权评估，但它们被视为实现隐私权立法规定合规性的最佳实践。如前面第 1 部分所述，根据这一点，财政委员会制定了一些政策工具和文件，包括 PIA 政策、PIA 指南、PIA 报告模板、PIA 最佳实践报告、PIA 电子学习工具、PIA 审计指南。实施 PIA 的政策责任在于中央机构，即加拿大财政委员会秘书处（TBS）。财政委员会秘书处不仅向财政委员会提供建议，并就政府如何在计划和服务上花钱、如何监管以及如何管理等方面提供建议，而且帮助确保政府为加拿大人明智而有效地花费税款[28]。财政委员会秘书处有 18 个下属部门，负责政府隐私政策的中央机构是隶属加拿大财政部秘书处首席信息官处的信息和隐私政策司，负责管理和解释政策，并向各机构、财政委员会主席和财务委员会提供建议。它的任务是制定和维持指导方针，以协助各机构执行该政策，并负责监测遵守情况。根据《金融管理法》第 7 条（财政委员会的职责和权力）[29]以及《隐私法》第 71(1)(d)条，财政委员会主席是负责政府立法管理的部长。财政委员会秘书处作为牵头机构，在立法修正方面与司法部合作，并在内阁机密事务上与隐私委员会办公室（Privay Council Office）合作。

2.3 政策内容

2.3.1 PIA 指导原则

根据《PIA 暂行指令》，PIA 指导原则包括 10 条，通常称为“公平信息原则”（见表 3），并在《加拿大标准协会保护个人信息的标准守则》中得到阐明。这些原则也被包含在《个人信息保护和电子文档法》（PIPEDA）中。

表 3 PIA 指导原则[30]

指导原则	内涵
问责制	组织负责其控制的个人信息,并应指定个人来负责确保组织遵守以下原则
识别目的	组织应在收集信息时或之前确定收集个人信息的目的
同意	除非有适当的情况,否则收集、使用或披露个人信息需要征得个人的同意
限制收集	个人信息的收集应限于组织确定的目的;信息应通过公平合法的方式得到收集
限制使用,披露和保留	除非获得个人同意或法律允许,否则不得将个人信息用于收集目的之外的目的或用途;仅在实现这些目的所必需的时间内保留个人信息
准确性	个人信息必须准确、完整和最新
保障措施	个人信息应得到适合其敏感性的安全保障措施的保护
开放性	组织应向个人提供有关其与个人信息管理相关的政策和实践的特定信息
个人获取	应告知个人其个人信息的存在、使用和披露,并应允许其获取该信息。个人应能够质疑信息的准确性和完整性,并对其进行适当的修改
挑战合规性	个人应能够向指定的一个或多个负责组织合规性的个人应对有关遵守上述原则的挑战

2.3.2 PIA 流程

《PIA 指南:管理隐私风险的框架》[6]有 3 个附件提供了 PIA 目录、PPIA 目录和汇总表示例。PIA 包括 4 个步骤:①项目启动。确定 PIA 的范围,并使指南中提供的工具适应具体情况。如果具体项目处于早期概念或设计阶段,而尚不清楚详细信息,则部门和机构应考虑进行初步隐私影响评估(PPIA)。一旦该项目发展并且存在隐私风险,就要求部门和机构进行完整的 PIA。在不寻常的情况下也可以进行初步的 PIA,在这些情况下,在审查政策和指南并获得专家建议后,对于 PIA 的需求仍然不明确。PIA 是一个动态过程,随着业务流程中设计的变化,PIA 也应进行审查和更新。②数据流分析。该活动包括对提议所考虑的业务流程、体系结构和详细数据流的描述和分析。此步骤的目的是描述个人信息流。③隐私权分析。隐私分析在适用的隐私政策和法规的背景下检查数据流。问卷用作检查清单,可帮助评估主体识别与提议的方案相关的主要隐私风险或漏洞。指南中提供了两套问卷,可以参阅问卷 A 的附件中的联邦计划和服务,以及问卷 B 的跨辖区倡议。④隐私影响分析报告。基于先前步骤的结果,这是 PIA 过程的最后也是最关键的组成部分。这是对隐私风险及其风险的相关评估的书面评估,并讨论可能的补救措施或缓解策略。

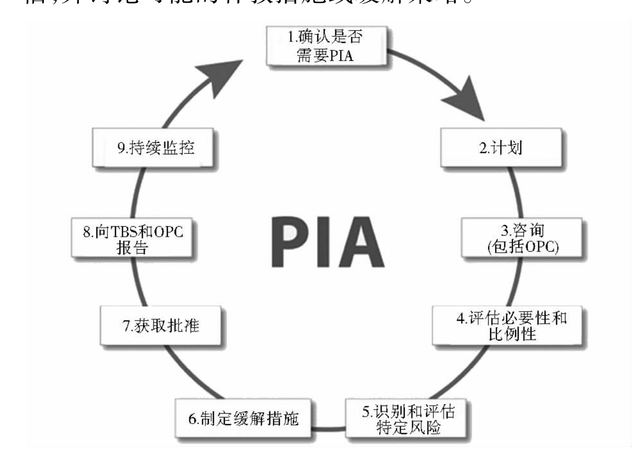


图 1 PIA 流程[18]

注:TBS 为财政委员会秘书处;OPC 为隐私专员办公室;PIA 为隐私影响评估

后来,2020 年 3 月修订后的《期望:向加拿大隐私专员办公室提交 PIA 的指南》对 PIA 流程进行更新(见图 2),内容包括:确认是否需要 PIA;计划;咨询(包括 OPC);评估必要性和比例性;识别和评估特定风险;制定缓解措施;获得批准;向财政委员会秘书处(TBS)和隐私专员办公室(OPC)报告;持续监控。

2.3.3 PIA 适用情形

图 2 可以帮助评估主体确定程序或活动的潜在隐私影响,并了解风险级别。基于此评估,即使没有以管理目的而使用个人信息,机构也可以选择进行 PIA。机构应单独考虑每个项目,以决定是否需要进行 PIA。

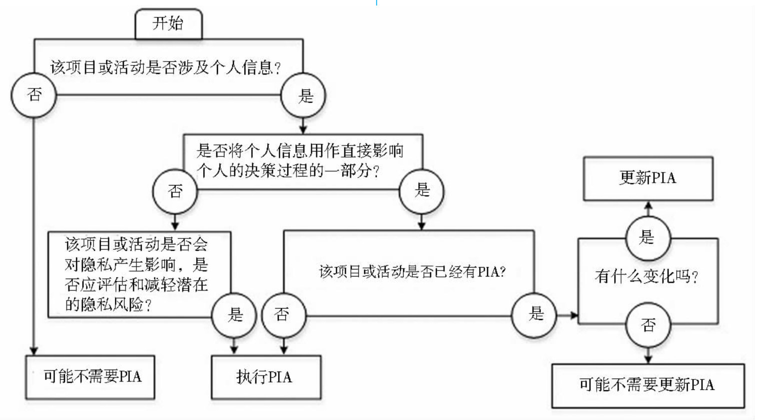


图 2 确定是否需要执行 PIA 的流程[18]

此外，根据《PIA 暂行指令》第 6.3.1 条，在以下情况下要针对项目或活动进行 PIA：当个人信息用于或打算用作直接影响个人的决策过程的一部分时；在对现有项目或活动进行实质性修改后，将个人信息用于或打算用于管理目的；将项目或活动外包或转移到另一级政府或私营部门时，会对项目或活动进行实质性修改。此外，《PIA 暂行指令》6.3.2 条还规定，与负责官员协商，确定一个全新或经过全面修改的信息处理计划或活动是否对隐私产生影响，并保证进行 PIA；政府机构的隐私协议足以解决此类程序或活动对隐私的潜在影响。可见，以上 5 种情况需要考虑进行 PIA。

2.3.4 PIA 规制对象

在加拿大中央政府层面，财政部委员会的政策要求，各部门和机构对所有涉及隐私问题的新方案和服务的提案进行 PIA。该政策适用于《隐私法》附表所列的所有政府机构，但加拿大银行除外。具体而言，这些机构包括加拿大国家部门和部委，以及一系列与政府有关的机构，包括大多数皇家公司（如加拿大土地有限公司、加拿大邮政公司、加拿大电视电影公司）、联邦机构（如加拿大交通局、加拿大税务局）和其它全部或部分由政府任命的机构（如加拿大小麦委员会）。

3 加拿大中央政府 PIA 政策分析

3.1 优势分析

3.1.1 完善政策法规以加强应用

在加拿大，PIA 是政策要求，而并非法律义务。因此，加拿大注重为 PIA 提供法律依据，并通过完善法律法规来提升 PIA 政策效力。例如，根据《PIA 暂行指令》3.4 条，本指令是根据《隐私法》第 71(1)(d)段和第 71(3)、71(4)、71(5)和 71(6)条发布的；根据第 3.5 条，本指令应与《隐私法》《隐私条例》《隐私保护临时政策》《隐私惯例暂行指令》《隐私请求和个人信息更正指令》[31] 以及《社会保险号码指令》[32] 一起阅读。为了提升法律支撑，财政委员会秘书处还发起并促进与 OPC 就 PIA 政策事项进行磋商。例如，PIPEDA 没有规定要强制性进行 PIA。类似地，通常而言，除非存在数据或信息匹配计划，否则新西兰《隐私法》也并未强制性规定要进行 PIA[33]。因此，2020 年 1 月 28 日，加拿大 OPC 发起了一次磋商，在磋商中提出了一些增强 PIPEDA 在人工智能系统中的应用和监管的建议。OPC 建议提高法律对透明度的要求，以授权进 PIA 的要求，包括与 AI 处理对隐私和人权的影响有关的评估[34]。

3.1.2 专职专责强化监管力量

在加拿大，PIA 的法律依据是在部级签发的文书，而且相关 PIA 政策是根据《隐私法》第 71(1)条而发布。《隐私法》第 71(1)条规定：根据第(2)(d)款的规定，指定部长应安排编制并向政府机构分发有关本法案和条例实施的指令和指南。根据《隐私法》第 3(1)条的规定，财政委员会主席已被指定为该法某些章节中所指的部长。通过优化财政委员会的专职专责，从而进一步明确它在 PIA 中管控工作的职责。例如，财政委员会将 PIA 定义为“确定提议对个人隐私的影响以及减轻或避免任何不利影响的方法的过程”。此外，这个机构也关注政策绩效，如财政委员会秘书处在《PIA 政策》生效后的 5 年内对其条款和运作进行全面审查[5]。如此，《PIA 政策》不仅使机构有责任证明其收集和使用个人信息尊重 1983 年的《隐私法》以及 2000 年的《个人信息保护和电子文档法》(PIPEDA)，而且还责令政府机构与公民进行交流为何收集他们的个人信息、如何使用和披露它们以及如何解决隐私影响的问题。

3.1.3 注重多主体合作

加拿大注重合作，如《PIA 暂行指令》第 6.3.4、6.3.5、6.3.6、6.3.7、6.3.8 条针对涉及多个机构的 PIA 情况进行规范：在涉及两个或多个政府机构的项目执行机构的情况下，该指令倾向于由一个机构牵头，并设想由关键（政府）利益相关者组成的部门间协调委员会。它倾向于一个单一、整体或多机构的项目执行机构，而不是由个别部门进行的独立项目执行机构。就 PIA 具体操作而言，PIA 由加拿大隐私专员办公室的审计和合规工作人员进行审查，后者不批准或拒绝，但对所采取的过程的质量提出意见。同样地，根据《PIA 暂行指令》第 8.1.1 条，财政委员会秘书处还将及时检查已批准的核心 PIA 的内容，以确保评估完成。财政委员会秘书处不批准 PIA，而仅审核核心 PIA，以履行其对 PIB 的审核和批准的义务。不过，根据《PIA 暂行指令》第 8.1.4 条，财政委员会秘书处每年审查附录 C 中的“核心 PIA”，以确保核心 PIA 保持相关性，并在需要时提出修订建议。以上可以看出，隐私专员办公室和财政委员会秘书处负责审查 PIA，但不批准 PIA。为了弥补这一职责空白，根据《PIA 暂行指令》文件的第 6.1 条，政府机构负责人负责建立 PIA 开发和

批准流程,并确保由机构内负责新的或经过重大修改的计划或活动的高级官员或执行人员完成 PIA。此外,《PIA 暂行指令》将 PIA 与提交给财政委员会的项目审批和资金筹措联系起来,这也是加拿大 PIA 政策的最显著特点之一。

3.2 劣势分析

公共政策具有主观性与不确定性。PIA 政策是政策设计者通过相应部门的行为而实现其目标,因而这一政策是否成功,取决于 PIA 政策设计和执行。PIA 政策的模糊性不仅限制目标,也影响政策手段。总体来看,加拿大 PIA 政策在目标、规范、执行方面存在模糊。

3.2.1 PIA 政策目标设定模糊

由于对政府服务提供过程中未来隐私问题的影响和成本的担忧,财政部委员会被赋予了制定《PIA 政策》的任务,以作为一种管理工具:确保在项目或服务的设计或重新设计过程中考虑隐私;评估将确定提案在多大程度上符合所有适当的法规;评估帮助管理者和决策者避免或减轻隐私风险,并促进充分知情的政策、计划和系统设计选择[5]。同样地,根据《PIA 暂行指令》附录 C,"核心 PIA"由与政策和法律合规性直接相关的 PIA 标准化要素组成。可见,这可以解释为 PIA 只是一种合规性的行为,但这可能是一种不公平的解释,因为如上所述,该指令将 PIA 视为风险管理的一部分,即使项目符合法律,也可能产生风险。

3.2.2 PIA 政策规范模糊

尽管加拿大的 PIA 具有对政府机构强制性的优点,但有关何时以及如何与利益相关者进行协商的指导方针尚不明确。同样地,也不清楚为什么只将 PIA 的摘要发布在机构的网站上,而不是像英国和美国的 PIA 政策中问题清单功能那样完整地发布 PIA,但用户可能会想查看这样的清单,尤其是那些仅要求是否做出回应的行为,因为与风险评估的实际需求不一致的方式"愚弄"了 PIA 概念。例如,美国各个政府部门都从 PIA 的标准化和工具性管理理念上,建立个人隐私保护指南,用可识别的方式对收集、储存、保护、分享和管理信息进行分析,以确保系统的使用者和相关组织有意识地将个人隐私纳入到一个系统的生命周期管理当中[35]。

3.2.3 PIA 政策执行模糊

加拿大 PIA 政策要求,加拿大各部门和机构必须向隐私专员提供评估结果的副本,并以英语和法语两种官方语言发布评估结果摘要,并应考虑定期出版和因特网出版。政府可以对这些摘要中的信息进行调整,以删除相关法律规定不能发布的信息或那些可能会使系统或安全措施变得脆弱的信息。但是,在实践过程中,各部门因未能公布隐私影响评估的执行结果和隐私影响评估报告的信息质量而达不到要求。

4 相关政策建议

4.1 提高政策执行人员技能

PIA 是一种可以被任何处理个人信息的机构使用的技术,尤其是政府,因为技术部门更适合政府。进行评估和完成隐私影响报告需要各种各样的技能,但一个人不必掌握全部的技能。进行评估的人员不仅需要具备良好的分析和写作能力,还需要熟悉信息隐私和数据保护方法。如果个人不具备相关的技术技能或经验,评估人员需要能够吸收与项目相关的文书工作,并能够与技术人员相处,提出相关问题,能够理解答案并将其转化为其他人能够理解的 PIA 报告。对于一个组织而言,一个善于探究的头脑和"横向"思考的才能是很有价值的。可见,为了提高 PIA 政策执行,可以从如下方面入手:①应当吸纳擅长如下技能的主体:政策制定、运营计划和业务设计、技术和专业知识、风险和合规性分析、程序和法律。②为了减小政策执行人员的"PIA 技能差距",建议鼓励各部门共享 PIA 工具、模板和框架。③建议向政策执行人员提供更多的培训和指导,使他们认识到在 PIA 政策中的责任,并为他们提供进行 PIA 所需的知识和技能。该过程包括规划、分析和教育活动,以及具有多种技能,以识别和评估隐私影响。这些技能包括隐私专业知识、法律专业知识、业务方案和业务设计技能、技术和系统专业知识以及信息和记录保存技能。

4.2 尽早制定 PIA 政策

每当有新的或实质性改变的电子政务项目时,组织都应完成项目影响评估。在项目开发的早期进行 PIA 是最有用的,因为它们可以在设计阶段用于识别风险和解决隐私问题。延迟 PIA 的组织有可能不得不对计划进行昂贵和耗时的更改,以确保其符合个人隐私保护法律法规。PIA 使公共和私人机构能够做出明智的选择。通常情况下,如果在项目规划的早期就确定了增强隐私的解决方案,那么实施该方案的难度和

成本不会比其它解决方案高。PIA 表明,从系统开发的初始阶段和整个信息的生命周期(即收集、使用、保留、处理、披露以及销毁)就考虑隐私,能确保隐私保护从一开始就被植入到系统中,而不是事后,因为这样做的代价可能要高得多,或者可能会影响项目的可行性。此外,PIA 还表明,系统开发人员和所有者已经做出了技术选择,反映了将隐私纳入基本系统架构的情况。

近年来,随着个人信息泄露事件频繁爆发,中国开始不断展开个人隐私保护制度设计。2020 年 5 月 25 日,全国人大常委会工作报告在下一步主要工作安排中指出,今年将围绕国家安全和社会治理,制定个人信息保护法、数据安全法[36]。2020 年 5 月 28 日,第十三届全国人民代表大会第三次会议通过了《中华人民共和国民法典》人格权编的第六章名为“隐私权和个人信息保护”,总结我国既有立法经验(如《网络安全法》)和学界通说确立了隐私权和个人信息保护的基本规则[37]。2020 年 7 月 22 日,最高法联合国家发改委,共同发布《关于为新时代加快完善社会主义市场经济体制提供司法服务和保障的意见》,明确要加强数据权利和个人信息安全保护,依法保护数据收集、使用、交易以及由此产生的智力成果,完善数据保护法律制度[38]。2020 年 10 月 13 日,备受关注的个人信息保护法草案提请十三届全国人大常委会第二十二次会议审议,规定对处理敏感个人信息等高风险处理活动,事前进行风险评估[39]。《信息安全技术 个人信息安全影响评估指南》指出,它是《个人信息安全规范》的配套标准,借鉴美、欧等国家和地区在个人信息安全影响评估(国际上习惯称为隐私影响评估(PIA))方面最新的法律规定、制度设计、实践做法,以国内现有立法、行政法规、标准要求为出发点,提出科学有效符合、信息化发展需要、具有明确实施指导意义的个人信息安全影响评估指南[40]。即便如此,这个文件也并非强制性标准,因而建议我国在《个人信息保护法》或《数据安全法》中进一步完善 PIA 的相关规范。就政策内容而言,应当包括适用情形、规制对象、隐私风险评估模型、事先咨询义务;就政策制定主体而言,应当吸收人大、政府、公民等政策活动者,从而确定数据控制者的 PIA 义务。

4.3 加强 PIA 政策认同

尽管加拿大 PIA 政策的主要目的是确保隐私保护在项目目标和活动的初始框架中是一个关键考虑因素,但即便在有些情况下有证据表明计划或服务交付可能会产生隐私问题,PIA 可能依旧根本无法完成。虽然隐私问题在政府 IT 项目的威胁和风险分析中明显显现出来,对于涉及机构间和跨区域的个人信息流动的项目,隐私保护的考虑要少得多。一些加拿大政府机构已经积极努力来实施 PIA 政策,但还需要更多的努力来确保政策达到预期效果,也就是说,提高对 PIA 政策中与项目和服务交付相关的隐私影响的认识和理解。因此,一方面,需要提高对 PIA 的认识。认知属于精神层面,能够有效预测满足与认同。通过提高对 PIA 政策的认知,从而通过相关价值评估形成信念后,会直接影响 PIA 政策的认同度。对具体机构来说,有许多益处:PIA 允许机构充分评估其信息共享计划中的隐私风险;它为制定全面有效的信息保护政策奠定了基础,同时最大限度地利用技术基础设施和数据共享机会;PIA 帮助组织审查提议计划的意图,识别和防止超出信息搜集预期目的的扩展,审查和接受风险,制定政策,并确定组织中负责处理个人信息的职位;它们还创建文档,根据要求告知个人其个人信息收集、使用和披露的地点和时间。另一方面,政策制定主体需要全面认定诸如数据控制者、数据利用者等 PIA 政策的利益相关者,从而制定符合公平正义的 PIA 政策,提高政策主体对 PIA 政策的支持与认同。这是因为,作为一项政策,PIA 政策会涉及不同的利益相关者,而它们会基于自身特质,分别诉求自身利益,但不同的利益相关者可能获得利益,但也可能有相应损失。

参考文献:

[1] 相丽玲,张轩瑜. 中外用户隐私影响评估标准比较[J/OL]. 情报理论与实践. [2021 – 06 – 27]. https://kns. cnki. net/kcms/detail/11. 1762. G3. 20210301. 1633. 004. tml.

[2] 崔聪聪, 许智鑫. 数据保护影响评估制度:欧盟立法与中国方案[J]. 图书情报工作, 2020,64(5):43 – 51.

[3] 陈朝兵,郝文强. 作为政府工具的隐私影响评估:缘起、价值、实施与启示[J]. 中国行政管理,2020(2):144 – 151.

[4] Annual report to parliament 1999 – 2000[EB/OL]. [2021 – 06 – 27]. https://www. priv. gc. ca/en/opc-actions-and-decisions/ar_index/02_04_08/.

[5] Privacy impact assessment policy[EB/OL]. [2021 – 06 – 27]. https://www. tbs-sct. gc. ca/pol/doc-eng. aspx? id = 12450.

[6] Treasury board of canada secretariat. Privacy impact assessment guidelines: a framework to manage privacy risks[EB/OL]. [2021 – 06 – 27]. http://www. tbs-sct. gc. ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld-PR-eng. asp? printable = True.

[7] Treasury board of canada secretariat. Preliminary privacy impact assessment template[EB/OL]. [2020-07-07]. http://www.tbs-sct.gc.ca/pgol-pged/ppia-epfvp/prelim-temp-modl/prelim-temp-modl00-eng.asp.
[8] Treasury board of canada secretariat. Reporton pia best practices [EB/OL]. [2020-07-14]. http://www.tbs-sct.gc.ca/pgol-pged/pia-best/pia-bestpr-eng.asp? format=print.
[9] Treasury board of canada secretariat. PIA e-learning tool[EB/OL]. [2020-07-26]. http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-eng.asp.
[10] Privacy act[EB/OL]. [2020-08-12]. https://laws-lois.justice.gc.ca/PDF/P-21.pdf.
[11] Personal information protection and electronic documents act (pipeda) (canada) [EB/OL]. [2020-08-14]. http://laws.justice.gc.ca/en/showdoc/cs/P-8.6//20090821/en? command=search&caller=SI&search_type=all&shorttitle=Personal%20information%20protection%20and%20electronic%20documents%20act&day=21&month=8&year=2009&search_domain=cs&showall=L&statuteyear=all&lengthannual=50&length=50. Accessed on: 21 August 2009.
[12] Treasury Board of Canada Secretariat. Privacy impact assessment audit guide[EB/OL]. [2020-09-14]. http://www.collectionscanada.gc.ca/webarchives/20071211001631/www.tbs-sct.gc.ca/ia-vi/policies-politiques/pia-efvp/pia-efvp_e.asp.
[13] Privacy and data protection policy[EB/OL]. [2020-10-11]. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/dwnld/chap1_1_e.rtf.
[14] Privacy regulations[EB/OL]. [2020-10-24]. https://laws-lois.justice.gc.ca/eng/regulations/SOR-83-508/index.html.
[15] Directive on privacy impact assessment[EB/OL]. [2020-11-14]. http://www.rogerclarke.com/DV/TBC-2010.pdf.
[16] Interim policy on privacy protection[EB/OL]. [2020-11-14]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx? id=12510.
[17] Interim directive on privacy practices[EB/OL]. [2020-11-24]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx? id=18309.
[18] Expectations: opc's guide to the privacy impact assessment process [EB/OL]. [2020-01-14]. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/#toc4-9.
[19] Office of the privacy commissioner of Canada[EB/OL]. [2020-10-13]. https://www.priv.gc.ca/en/.
[20] Privacy impact assessment[EB/OL]. [2020-10-06]. https://www.priv.gc.ca/en/opc-news/speeches/02_05_a_020508/.
[21] The role of the privacy impact assessment[EB/OL]. [2020-10-11]. https://www.priv.gc.ca/en/opc-news/speeches/2004/sp-d_040310/.
[22] The privacy impact assessment: your gps through the new landscape of privacy protection[EB/OL]. [2020-10-24]. https://www.priv.gc.ca/en/opc-news/speeches/2011/sp-d_20110928_cb/.
[23] Facing the breach: privacy and security as an ecosystem[EB/OL]. [2020-04-04]. https://www.priv.gc.ca/en/opc-news/speeches/2013/sp-d_20130618_cb/.
[24] A risk based approach for accountability and compliance[EB/OL]. [2020-04-15]. https://www.priv.gc.ca/en/opc-news/speeches/2013/sp-d_20130926_cb/.
[25] Working together as privacy champions[EB/OL]. [2020-04-26]. https://www.priv.gc.ca/en/opc-news/speeches/2014/sp-d_20141210/.
[26] The interconnected worlds of privacy and cyber-security[EB/OL]. [2020-05-04]. https://www.priv.gc.ca/en/opc-news/speeches/2016/sp-d_20160420/.
[27] Modernizing federal privacy laws to better protect canadians[EB/OL]. [2020-05-11]. https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200309/.
[28] Treasury Board of Canada Secretariat[EB/OL]. [2020-05-19]. https://www.canada.ca/en/treasury-board-secretariat.html.
[29] Financial administration act-laws.justice.gc.ca[EB/OL]. [2020-05-26]. https://laws-lois.justice.gc.ca/eng/acts/f-11/page-2.html#h-228122.
[30] Personal information protection policy[EB/OL]. [2020-06-04]. https://www.ferocorp.com/pages/privacy.html.
[31] Directive on privacy requests and correction of personal information [EB/OL]. [2020-07-23]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx? id=18311.
[32] Directive on social insurance number[EB/OL]. [2020-08-11]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx? id=13342.
[33] 陈美,谭纬东. 政府开放数据的隐私风险评估与防控:新西兰的经验[J]. 情报理论与实践,2020,43(5):110-114,90.
[34] Consultation on the opc's proposals for ensuring appropriate regulation of artificial intelligence[EB/OL]. [2020-09-18]. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/.
[35] 周庆山. 完善我国个人信息保护管理制度的思考[J]. 社会治理, 2018(1):34-41.
[36] 重磅! 个人信息保护法、数据安全法终于要来了! [EB/OL]. [2020-10-16]. https://k.sina.com.cn/article_1750987934_685df49e01900mv0l.html? from=news&subch=onews.
[37] 民法典规定的隐私权和个人信息保护[EB/OL]. [2020-10-17]. http://m.workercn.cn/wq/2020/0804/200804093628350.shtml.
[38] 最高法、国家发改委发布意见:加强数据权利和个人信息安全保护[EB/OL]. [2020-10-18]. https://www.sohu.com/a/410614389_741570.
[39]《中华人民共和国个人信息保护法(草案)》首次亮相[EB/OL]. [2020-10-19]. https://www.sohu.com/a/424842464_

100014118.
[40]《个人信息安全影响评估指南》(GB/T 39335-2020) 正式发布[EB/OL]. [2021-06-05]. https://www.secrss.com/articles/27363.

作者贡献说明：
陈美：资料收集整理、撰写与修改论文；
梁乙凯：文献调研、资料收集整理。

Canadian Privacy Impact Assessment Policy: History, Content, Analysis and Implications

Chen Mei[1] Liang Yikai[2]
[1] School of Public Administration, Zhongnan University of Economics and Law, Wuhan 430073
[2] School of Management Science and Engineering, Shandong University of Finance and Economics, Jinan 250014

Abstract: [**Purpose/significance**] From the perspective of policy, this paper investigates the policy support of the privacy impact assessment in Canada to provide reference for the policy formulation of the privacy impact assessment in China and provide tools for the government to protect citizens' privacy. [**Method/process**] Using the research methods of literature research and case analysis, taking Canada as an example, this paper expounded the development process of the privacy impact assessment policy in Canada by obtaining first-hand materials through the investigation of literature and website contents, and sorted out the policy objectives, policy subjects and policy contents. On this basis, it analyzed the advantages and disadvantages of the privacy impact assessment policy in Canada. [**Result/conclusion**] This paper puts forward suggestions on improving the skills of policy executives, formulating PIA policies as early as possible, and strengthening the identification of PIA policies.

Keywords: privacy impact assessment Canada government open data privacy risk